الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1148

(2020/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

التطبيقات والخدمات الآمنة (1) – أمن الويب

إطار عملية إزالة المعرِّفات لمقدمي خدمات الاتصالات

التوصية ITU-T X.1148

الاتحاد الدولي للاتصالات ITU

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
أمن الشبكة	X.1030–X.1049
إدارة الأمن	X.1050–X.1069
الخصائص البيومترية	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المحلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن الويب	**X.1140–X.1149**
بروتوكولات الأمن (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
أمن معرفات الهوية عبر الشبكات	X.1170–X.1179
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
أمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	X.1230–X.1249
إدارة الهوية	X.1250–X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
أمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
أمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
أمن إنترنت الأشياء (IoT)	X.1360–X.1369
أمن أنظمة النقل الذكية (ITS)	X.1370–X.1389
أمن سجل الحسابات الموزع	X.1400–X.1429
أمن سجل الحسابات الموزع	X.1430–X.1449
البروتوكول الأمني (2)	X.1450–X.1459
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1500–X.1519
تبادل مواطن الضعف/الحالة	X.1520–X.1539
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل السياسات	X.1550–X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560–X.1569
تعرف الهوية والاكتشاف	X.1570–X.1579
التبادل المضمون	X.1580–X.1589
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1600–X.1601
تصميم أمن الحوسبة السحابية	X.1602–X.1639
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1640–X.1659
تنفيذ أمن الحوسبة السحابية	X.1660–X.1679
أمن أشكال أخرى للحوسبة السحابية	X.1680–X.1699
الاتصالات الكمومية	
المصطلحات	X.1700–X.1701
مولّد الأعداد العشوائية الكمومية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1710–X.1711
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1712–X.1719
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
أمن شبكات الجيل الخامس	X.1800–X.1819

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1148

إطار عملية إزالة المعرِّفات لمقدمي خدمات الاتصالات

ملخص

تقوم منظمات الاتصالات بجمع وإدارة واستخدام وتبادل بيانات عن الأفراد، بما في ذلك المعلومات المحددة لهوية الأشخاص. ونتيجة لذلك، فهي تستخدم تقنيات إزالة معرفات البيانات لحماية بيانات الأفراد. وتصف التوصية ITU-T X.1148 إطار عملية إزالة المعرِّفات بخطوات تشغيلية وتوصِّف نماذج إصدار البيانات ومراحل البيانات في عملية إزالة المعرِّفات لدى مقدمي خدمات الاتصالات بناءً على نموذج دورة حياة البيانات وأدوار أصحاب المصلحة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1148	2020-09-03	17	11.1002/1000/14249

مصطلحات أساسية

أساس البيانات، إزالة المعرِّفات، عملية إزالة المعرِّفات، إغفال الهوية-k، التنوع-l، حماية المعلومات المحددة لهوية الأشخاص، نماذج النشر، القرب-t

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

الصفحة

مقدمة

مع التطور السريع لتكنولوجيا وخدمات المعلومات والاتصالات القائمة على الإنترنت، تشهد الكمية الضخمة من البيانات المتولدة والمنقولة والمخزنة نمواً هائلاً. وتتولد البيانات من مصادر عديدة ليست حكراً على أجهزة الاستشعار أو الكاميرات أو أجهزة الشبكة، بل تشمل أيضاً صفحات الويب وأنظمة البريد الإلكتروني أو الشبكات الاجتماعية وغيرها الكثير. وأصبحت مجموعات البيانات أكبر وأعقد وأسرع قدوماً من قدرة طرق وأدوات معالجة البيانات التقليدية على مجاراتها. وصارت تحليلات البيانات بكفاءة في غضون تأخير محتمل صعبة للغاية. يجري تطوير أنموذج يسمى تحليلات البيانات الضخمة لحل المشكلات المذكورة أعلاه.

وتقوم منظمات الاتصالات بجمع وإدارة واستخدام وتبادل بيانات عن الأفراد، بما في ذلك المعلومات المحددة لهوية الأشخاص. ونتيجة لذلك، فهي تستخدم تقنيات إزالة معرفات البيانات لحماية بيانات الأفراد. والعلاقات بين الأطراف المشاركة في تدفق البيانات لتبادل البيانات تؤثر على ما إذا كانت هناك حاجة لإزالة معرفات البيانات قبل جمعها، أو بعد جمعها ولكن قبل تخزينها، أو فقط قبل إطلاع الطرف التالي في تبادل البيانات عليها. وبناءً على ذلك، يحتاج مقدمو خدمات الاتصالات إلى تقديم إزالة معرفات البيانات كخدمة في الوقت المناسب وبطريقة فعالة وآمنة لعملاء البيانات.

التوصية ITU-T X.1148

إطار عملية إزالة المعرِّفات لمقدمي خدمات الاتصالات

1 مجال التطبيق

تقدم هذه التوصية لمحة عامة عن عملية إزالة المعرِّفات بناءً على نموذج دورة حياة البيانات، وتوصِّف إطار عملية إزالة المعرِّفات بالخطوات والأدوار التشغيلية لأصحاب المصلحة في عملية إزالة المعرِّفات. وهي تتناول بالبحث أيضاً نماذج إصدار البيانات ومراحل البيانات في عملية إزالة المعرِّفات وتتضمن نُهجاً وأمثلة مختلفة لإزالة المعرِّفات في ملحقاتها وتذييلاتها.

ولا تتطرق هذه التوصية إلى القضايا المتعلقة بالتنظيم.

2 المراجع

لا توجد.

3 التعاريف

1.3 تعاريف معرفة في وثائق أخرى

تستخدم هذه التوصية التعاريف التالية المعرفة في وثائق أخرى:

1.1.3 البيانات المجمعة (aggregated data) [b-ISO/IEC 20889]: بيانات تمثل مجموعة من أسس البيانات، مثل مجموعة من الخصائص الإحصائية لتلك المجموعة.

2.1.3 إغفال الهوية (anonymization) [ISO/IEC 29100]: عملية يتم بواسطتها تغيير المعلومات PII بشكل نهائي وبطريقة لا يمكن معها التعرف على صاحب المعلومات PII بصورة مباشرة أو غير مباشرة، سواء من مراقب المعلومات PII وحده أو بالتعاون مع أي طرف آخر.

3.1.3 النعت (attribute) [b-ISO/IEC 20889]: السمة المتأصلة.

4.1.3 مجموعة البيانات (dataset) [b-ISO/IEC 20889]: مجموعة من البيانات.

5.1.3 إزالة المعرِّفات (de-identification) [b-ISO 25237]: مصطلح عام لأي عملية تخفيف ارتباط بين مجموعة من البيانات المعرِّفة وموضوع هذه البيانات (انظر الفقرة 4.2.3).

6.1.3 إزالة المعرِّفات (de-identification process) [b-ISO/IEC 20889]: عملية إزالة الارتباط بين مجموعة من النعوت المعرِّفة وبين أساس البيانات.

7.1.3 تقنية إزالة المعرِّفات (de-identification technique) [b-ISO/IEC 20889]: أسلوب لتحويل مجموعة بيانات بهدف تقليل مدى إمكانية ربط المعلومات بفرادى أسس البيانات.

8.1.3 مجموعة بيانات مجرَّدة من المعرِّفات (de-identified dataset) [b-ISO/IEC 20889]: مجموعة بيانات ناتجة عن تطبيق عملية إزالة المعرِّفات.

9.1.3 المعلومات المجرَّدة من المعرِّفات (de-identified information) [b-NISTIR 8053]: سجل أزيل عنه أو حُجب فيه ما يكفي من المعلومات المحددة لهوية الأشخاص بحيث لا تحدد المعلومات المتبقية هوية الفرد ولا يوجد أساس معقول للاعتقاد بإمكانية استخدام المعلومات لتحديد هوية فرد.

10.1.3 الخصوصية التفاضلية (differential privacy) [b-ISO/IEC 20889]: نموذج قياس خصوصية رسمي يضمن أن يختلف التوزيع الاحتمالي للمخرجات عن التحليل الإحصائي بقيمة محددة على الأكثر، سواء ورد أو لم يرد تمثيل لأي أساس بيانات معين في مجموعة بيانات المدخلات.

ملاحظة – بعبارة أدق، تقدم الخصوصية التفاضلية ما يلي:

أ) تعريف رياضي للخصوصية يفترض أن اعتبار نتائج أي تحليل إحصائي حافظة للخصوصية، يستلزم تعذر تمييز نتائج التحليل من مجموعة البيانات الأصلية عن تلك التي المحصَّلة في حال إضافة أي أساس بيانات إلى مجموعة البيانات أو إزالته منها؛

ب) مقياس للخصوصية يتيح مراقبة الخسارة التراكمية للخصوصية وتحديد الحد الأعلى لمدى الخسارة (أو "ميزانيتها"). ويرد تعريف رسمي كما يلي. ليكن ε رقماً حقيقياً موجباً، ولتكن M خوارزمية عشوائية تأخذ مجموعة بيانات كمدخلات. فيُقال إن الخوارزمية M خاصة تفاضلياً إذا اختلفت في كل مجموعات البيانات D1 وD2 ضمن عنصر واحد (أي بيانات مصدر بيانات واحد)، وجميع المجموعات الفرعية S لمدى الخوارزمية M، mml_m1، حيث يطغى الاحتمال على العشوائية التي تستخدمها الخوارزمية.

11.1.3 المعرِّف (identifier) [b-ISO/IEC 20889]: مجموعة من النعوت في مجموعة بيانات تتيح تعرفاً ينفرد به أساس البيانات ضمن سياق تشغيلي محدد.

ملاحظة – انظر الملحق B للاطلاع على بحث بشأن كيفية ارتباط هذا التعريف بالتعاريف الواردة في المعايير الأخرى.

12.1.3 النعت المعرِّف (identifying attribute) [b-ISO/IEC 20889]: نعت في مجموعة بيانات يمكن أن يساهم في تعرُّف تنفرد به البيانات في سياق تشغيلي محدد.

13.1.3 صاحب الخصوصية (privacy stakeholder) [b-ISO/IEC 29100]: شخص طبيعي أو اعتباري أو سلطة عامة أو وكالة أو أي هيئة أخرى يمكن أن تؤثر أو تتأثر أو تتصور أنها تتأثر بقرار أو نشاط يتعلق بمعالجة المعلومات المحددة لهوية الأشخاص (PII).

14.1.3 استخدام اسم مستعار (pseudonymization) [b-ISO/IEC 20889]: تقنية إزالة معرّفات تبدل معرّفاً (أو معرّفات) لأساس بيانات باسم مستعار لإخفاء هوية أساس البيانات هذا.

15.1.3 شبه المعرّف (quasi-identifier) [b-ISO/IEC 20889]: نعت في مجموعة بيانات يفرز أساس البيانات، عندما يؤخذ هذا النعت في الاعتبار بالاقتران مع نعوت أخرى في مجموعة البيانات.

16.1.3 السجل (record) [b-ISO/IEC 20889]: مجموعة من النعوت المتعلقة بأساس بيانات واحد.

17.1.3 إعادة المعرِّفات (re-identification) [b-ISO/IEC 20889]: عملية ربط البيانات في مجموعة بيانات مجرَّدة من المعرِّفات بأساس البيانات الأصلي.

ملاحظة – ترد في هذا التعريف عملية تثبت وجود أساس بيانات معين في مجموعة بيانات.

18.1.3 فرز (single out) [b-ISO/IEC 20889]: عزل السجلات العائدة إلى أساس البيانات في مجموعة بيانات من خلال رصد مجموعة من الخصائص يُعلم أنها تخص أساس البيانات دون غيره.

19.1.3 الطرف الثالث (third party) [b-ISO/IEC 29100]: صاحب الخصوصية بخلاف مدير المعلومات المحددة لهوية الأشخاص (PII)، ومراقب المعلومات المحددة لهوية الأشخاص ومعالج المعلومات المحددة لهوية الأشخاص، والأشخاص الطبيعيين المفوضين لمعالجة البيانات تحت السلطة المباشرة لمراقب المعلومات المحددة لهوية الأشخاص أو معالج المعلومات المحددة لهوية الأشخاص.

20.1.3 الطرف الثالث الموثوق (Trusted Third Party) [b-ISO/IEC 18014-1:2008]: سلطة أمن، أو وكيلها، تثق بها كيانات أخرى فيما يتعلق بالأنشطة المتصلة بالأمن.

21.1.3 إغفال الهوية–k (k-anonymity) [b-ISO/IEC 20889]: نموذج قياس خصوصية رسمي يضمن أن لكل معرف في مجموعة بيانات صنف تكافؤ مقابل يحتوي على سجلات لا يقل عددها عن K.

22.1.3 التنوع–l (l-diversity) [b-ISO/IEC 20889]: نموذج قياس خصوصية رسمي يضمن أن في النعت المختار، يحتوي كل صنف تكافؤ على قيم ممثلَة جيداً لا يقل عددها عن L.

ملاحظة – التنوع–L هو خاصية لمجموعة البيانات تعطي حداً أدنى مضمون، L، بشأن تنوع القيم المشتركة بواسطة صنف تكافؤ لنعت محدد.

23.1.3 القُرب–t (t-closeness) [b-ISO/IEC 20889]: نموذج قياس خصوصية رسمي يضمن ألا تزيد المسافة بين توزيع النعت المختار في صنف تكافؤ وتوزيع هذا النعت في الجدول بأكمله عن العتبة T.

ملاحظة – يُقال إن للجدول القُرب–T فيما يتعلق بنعت مختار إذا كان لجميع أصناف التكافؤ التي تحتوي على هذا النعت القُرب–T.

2.3 تعاريف معرفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 مراقب البيانات (data controller): صاحب المصلحة (أو صاحب الخصوصية) الذي يحدد أغراض ووسائل معالجة البيانات بخلاف الأشخاص الطبيعيين الذين يستخدمون البيانات لأغراض شخصية.

2.2.3 معالج البيانات (data processor): صاحب مصلحة يعالج البيانات نيابةً عن مراقب البيانات ووفقاً لتعليماته.

3.2.3 مسؤول حماية البيانات (data protection officer): الشخص المعين من مراقب المعلومات المحددة لهوية الأشخاص (PII) لضمان الالتزام على نحو مستقل بمتطلبات قانون/لائحة الخصوصية.

ملاحظة – "مراقب المعلومات المحددة لهوية الأشخاص (PII)" هو مرادف لعبارة "مراقب البيانات".

4.2.3 موضوع البيانات (data subject): الكيان الذي تتعلق به البيانات.

ملاحظة – "موضوع البيانات" هو مرادف لعبارة "المعلومات المحددة لهوية الأشخاص" و"أساس البيانات".

5.2.3 العملية (process): فيما يتعلق بالمعلومات أو البيانات، إنها تعني الحصول على المعلومات أو البيانات أو تسجيلها أو الاحتفاظ بها أو تنفيذ أي تشغيل أو مجموعة من التشغيلات للمعلومات أو البيانات، بما في ذلك:

- تنظيم أو تكييف أو تغيير المعلومات أو البيانات،
- أو استخراج المعلومات أو البيانات أو الاطلاع عليها أو استخدامها،
- أو الكشف عن المعلومات أو البيانات عن طريق الإرسال أو النشر أو الإتاحة بأي شكل آخر،
- أو مواءمة أو دمج أو حجب أو محو أو إتلاف المعلومات أو البيانات.

4 المختصرات

تستعمل هذه التوصية المختصرات التالية:

DP الخصوصية التفاضلية *(Differential Privacy)*

DPO مسؤول حماية البيانات *(Data Protection Officer)*

PII المعلومات المحددة لهوية الأشخاص *(Personally Identifiable Information)*

TTP الطرف الثالث الموثوق *(Trusted Third Party)*

5 الاصطلاحات

لا يوجد.

6 نظرة عامة على عملية إزالة المعرِّفات

الغرض من عملية إزالة المعرِّفات هو إبقاء بيانات المواضيع طي الكتمان. ونظراً لأن هذه البيانات قد تشتمل على المعلومات المحددة لهوية الأشخاص، قبل وبعد تحليلات البيانات الرامية لاستخراج معلومات ذات معنى، تجب على محلل البيانات مراعاة اعتبارات الأمن.

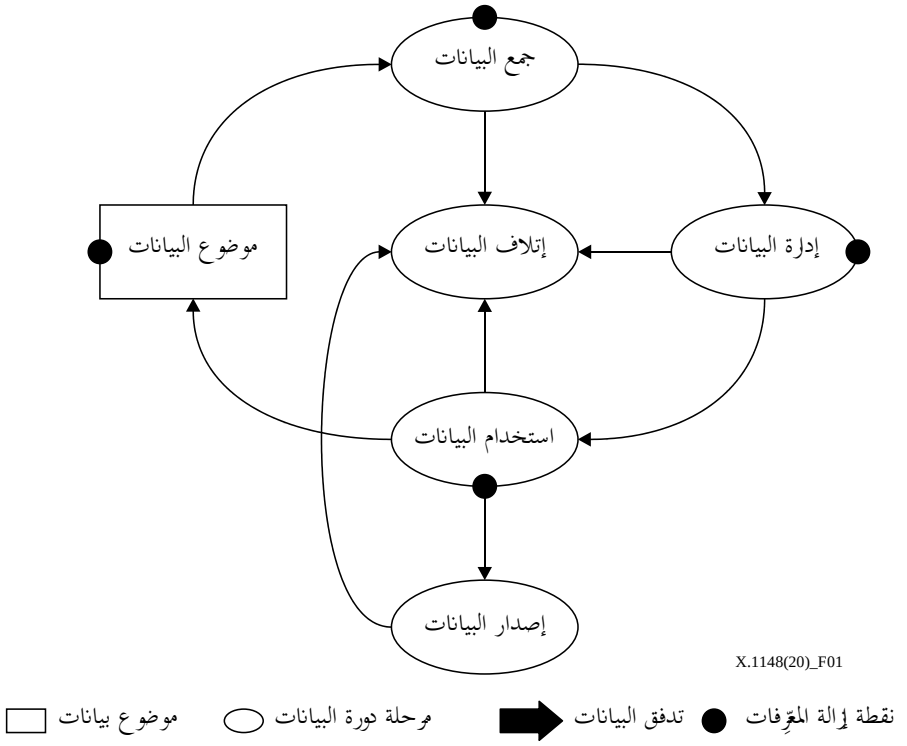
وتحدد هذه الفقرة بيئات تحليل البيانات، ونموذج دورة حياة البيانات، وأدوار الكيانات في عملية إزالة المعرِّفات واعتبارات أخرى في إزالة المعرِّفات.

1.6 نموذج دورة حياة البيانات ومرحلة إزالة المعرِّفات

عادةً ما تحدد المنظمة أهداف إزالة المعرِّفات وفق مقاصد الخصوصية والأمن. وتعرِّف هذه الفقرة دورة حياة البيانات وتصف متى يجب التفكير في عملية إزالة المعرِّفات بناءً على نموذج دورة حياة البيانات.

ويُستخدم مفهوم دورة حياة البيانات لتحديد الضوابط المناسبة بناءً على تحليل إمكانية إعادة المعرِّفات. وتعرِّف هذه التوصية دورة حياة البيانات المبينة في الفقرات من 1.1.6 إلى 5.1.6.

ويقدم الشكل 1 نظرة عامة على عملية إزالة المعرِّفات في نموذج دورة حياة البيانات.



الشكل 1 – عملية إزالة المعرِّفات في نموذج دورة حياة البيانات

1.1.6 مرحلة جمع البيانات

تُجمع البيانات من مواضيع البيانات وهي الأشخاص الذين تشير البيانات إليهم. ويمكن أن تتضمن مجموعة البيانات الناتجة عن جمع البيانات هذا معلومات محدِدة لهوية الأشخاص. وتنشئ إزالة المعرِّفات مجموعة بيانات جديدة أزيلت منها جميع المعلومات المحددة لهوية الأشخاص. ويوصى بأن تستخدم المنظمات مجموعات البيانات المجرَّدة من المعرِّفات داخلياً بدلاً من مجموعة البيانات الأصلية، حيثما أمكن ذلك.

وباستخدام هذا النموذج، تمكن إزالة المعرِّفات إما:

- أثناء جمع البيانات، أي (ب) في الشكل 1؛
- أو في حال جمع البيانات ولكن دون الحاجة إلى معرف بالفعل، أي (أ) في الشكل 1.

وينبغي عدم جمع المعرِّفات غير اللازمة لإدارة البيانات (تحويل البيانات والاحتفاظ بالبيانات).

2.1.6 مرحلة إدارة البيانات

لتجنب أرشفة المعرّف، ينبغي تطبيق إزالة المعرِّفات بعد تحويل البيانات وقبل الاحتفاظ بالبيانات، أي (ج) في الشكل 1. وتوصى المنظمات بالنظر في إمكانية إعادة المعرِّفات ووضع ضوابط نفاذ واضحة، وحدود قصوى للاحتفاظ بالبيانات، وسياسات إزالة بيانات تقلل إلى أقصى حد من إمكانية الربط بين البيانات المجرَّدة من المعرِّفات. وتوصى المنظمات بالنظر في تقنيات إغفال الهوية مثل تجميع البيانات، حيثما يسمح بذلك الغرض المقصود من الاستخدام.

3.1.6 مرحلة استخدام البيانات

إذا دعت الحاجة إلى معلومات محدِدة لهوية أشخاص (PII) داخل منظمة لإدارة البيانات، يوصى بإزالة معرِّفات البيانات قبل إصدارها كمجموعة بيانات لتبادل البيانات، أي (د) في الشكل 1.

4.1.6 مرحلة إصدار البيانات

يمكن تبادل البيانات مع أطراف ثالثة ملزَمة بضوابط إدارية إضافية مثل اتفاقات "تبادل البيانات". وقد تكون مجموعات البيانات المجرَّدة من المعرِّفات برسم الإصدار. ويصنَّف إصدار البيانات المجرَّدة من المعرِّفات في ثلاثة نماذج: عمومي أو شبه عمومي أو غير عمومي. ويمكن أن يختلف مقدار إزالة المعرِّفات المطلوب حسب نموذج الإصدار المختار.

5.1.6 مرحلة إتلاف البيانات

يمكن إتلاف البيانات في أي مرحلة، أي في مرحلة جمع البيانات، وإدارة البيانات، واستخدام البيانات، وإصدار البيانات. وينبغي إتلاف البيانات بتدابير جرى التحقق منها لتجنب استعادة البيانات. وعلى وجه الخصوص، ينبغي النظر في إتلاف البيانات عند كشف إمكانية إعادة المعرِّفات.

2.6 اعتبارات إزالة المعرِّفات

يؤدي تطبيق إزالة المعرِّفات طوال دورة حياة البيانات إلى زيادة فعاليتها. بيد أن طبيعة العلاقات بين الأطراف المشاركة في تدفق البيانات تؤثر على ما إذا كانت إزالة معرِّفات البيانات لازمة قبل جمعها، أي (أ) في الشكل 1، أو بعد جمعها، أي (ب) في الشكل 1، ولكن قبل الاحتفاظ بها، أي (ج) في الشكل 1، أو فقط قبل إطلاع الطرف التالي في تدفق البيانات عليها، أي (د) في الشكل 1. ويؤثر هذا القرار بدوره على جدوى الأمن وتدابير أخرى في المنظمة لتعزيز فعالية تقنية معينة لإزالة المعرِّفات في كل حالة استخدام. وعلى الرغم من أن إزالة المعرِّفات يمكن أن تكون تقنية مفيدة لإبقاء بيانات المواضيع طي الكتمان في الحالات التي لا يدعم فيها الغرض من الاستخدام تقنيات إغفال الهوية، إلا أنها ليست كافية في حد ذاتها لحماية بيانات المواضيع ويجب اعتبارها جزءاً من إطار شامل لحماية البيانات. وتصف هذه الفقرة ميزات واعتبارات كل مرحلة.

1.2.6 جمع البيانات

يعد إزالة المعرِّفات محلياً (أو إزالة المعرِّفات في المصدر) هو النهج الأبرز الذي يسمح لفرد (أو لمراقب يعالج بيانات لفرد) بإزالة جميع المعلومات المحددة لهوية الأشخاص قبل الإفراج عن البيانات للتحليلات.

وأحد جوانب إزالة المعرِّفات المرتبط مباشرة بمرحلة جمع البيانات هو تقليل البيانات إلى أدنى حد. فيُطلب من كل مراقب بيانات يقوم بجمع بيانات المواضيع تحديد البيانات الضرورية تماماً لغرض الاستخدام المقصود، وقصر جمع البيانات على تلك المعلمات المحددة حصراً.

وينبغي أن تكون هناك عمليات محددة لاستبعاد المعلومات المحددة لهوية الأشخاص غير الضرورية من جمع/نقل البيانات، من أجل تقليل حقول البيانات.

ويتمثل جانب آخر من إزالة المعرِّفات في تجميع البيانات. فيُطلب من مراقبي البيانات النظر في تجميع البيانات في جميع الحالات التي لا يتطلب فيها الغرض من الاستخدام تماماً فرز فرادى مواضيع البيانات.

2.2.6 إدارة البيانات

1.2.2.6 تحويل البيانات

يمكن أن تتضمن مرحلة تحويل البيانات تطبيق تقنيات إزالة المعرِّفات مثل التجميع، والحد من الكشف الإحصائي، والتجفير، وما إلى ذلك. ويمكن تطبيق تحويل البيانات في مرحلة واحدة أو عدة مراحل، بما في ذلك مباشرة بعد التجميع وقبل الاحتفاظ لفترة طويلة، أو بعد الاحتفاظ لفترة طويلة وقبل النفاذ، أو دمجاً مع النفاذ.

ويمكن استخدام التحويل المشترك لتنقيح البيانات أو تجميعها في أي وقت بعد جمعها وحتى إصدارها. فإذا طُبِّق مباشرة بعد الجمع أو يمكن لتنقيح البيانات أو تجميعها أن يقلل من الضرر المحتمل لمواضيع البيانات في حالة خرق البيانات؛ ولكن ذلك يؤدي أيضاً إلى الحد من إمكانية ربط البيانات أو دمجها أو تحديثها بعد التنقيح.

وينبغي اختيار أسلوب تحويل البيانات بعد دراسة متأنية للضرر المحتمل المتمثل في إفشاء مواضيع البيانات. وينبغي أن يأخذ قرار التحويل في الحسبان أيضاً التحليلات التي يجب دعمها بغرض استخدام البيانات لاحقاً، لأن التقنيات المستخدمة للحد من مخاطر الكشف يمكن أن تؤثر على إمكانية الاستخدامات والتحليلات اللاحقة.

2.2.2.6 الاحتفاظ بالبيانات

يوصف الاحتفاظ بالبيانات بأنه عملية تخزين البيانات، بما فيها المعلومات المحددة لهوية الأشخاص (PII)، في أي شكل من أشكال التخزين غير المتغير بواسطة مراقب البيانات أو طرف يعمل تحت توجيه المراقب. وتركز ضوابط أمن المعلومات والخصوصية بالفعل على مرحلة الاحتفاظ، وبالتالي تلخص هذه الفقرة الضوابط دون تقديم اعتبارات تفصيلية [b-ISO/IEC 27001]. ويشيع عدد من ضوابط أمن المعلومات والخصوصية في مرحلة الاحتفاظ، مثل التحكم في النفاذ، والصيانة، وتقييمات الأمن، وإجراءات الاستيقان، ومراقبة الحوادث والاستجابة لها، وعمليات التدقيق.

وعلى وجه الخصوص، ينبغي للمنظمات اتباع الحد الأقصى من سياسات الاحتفاظ بالبيانات وإزالتها لضمان الاحتفاظ بالبيانات لفترة لا تزيد عما هو ضروري تماماً لتحقيق الغرض من الاستخدام، وإتلاف البيانات تماماً بعد فترة الاحتفاظ القصوى هذه. فعلى سبيل المثال، كثيراً ما تنص اتفاقات تبادل البيانات على وجوب أن يتلف المستلم البيانات في غضون فترة زمنية محددة، مثل سنة واحدة بعد الاستلام، وقد تتطلب القوانين أيضاً مثل هذا الحكم التعاقدي.

3.2.6 استخدام البيانات

يمكن جمع البيانات المجرَّدة من المعرِّفات أو تخزينها أو تبادلها لمجموعة من الأغراض والتطبيقات، يعتمد كل منها على خصائص بيانات معينة تُحفظ بعد إزالة المعرِّفات. ويكمن أحد الأسباب الرئيسية للإفراج عن مجموعات البيانات المجرَّدة من المعرِّفات في إتاحة الفرصة للآخرين لدراسة قيم وخصائص البيانات الخام لأغراض البحث [b-ISO/IEC 20889]. لذلك، ينبغي أن تسعى إزالة المعرِّفات أيضاً إلى الحفاظ على أكبر قدر ممكن من الفائدة في المعلومات، مع حماية خصوصية الأفراد. ويجعل هذا الغرض المزدوج من إزالة المعرِّفات نهجاً مهماً للنظر في استخدامه في عدد من السياقات، بما في ذلك نماذج إصدار البيانات.

وعند إصدار بيانات مجرَّدة من المعرِّفات، يجب على المنظمة اتخاذ قرار، تتخذه عادةً لجنة خبراء تتضمن مجموعة واسعة من أصحاب المصلحة، للنظر في التأثيرات المحتملة على مواضيع البيانات المتعلقة بالإصدار. وكثيراً ما تُستخدم تقديرات المخاطر وقوائم المراجعة لتوجيه هذا التقييم وتحديد آلية إصدار مناسبة تخفف من مخاطر إعادة المعرِّفات.

ويعتمد اختيار تقنيات إزالة المعرِّفات على درجة قابليتها للتطبيق أو "قيمتها الاستعمالية" في حالة استخدام معينة.

7 إطار عملية إزالة المعرِّفات

تصف هذه الفقرة إطار عملية إزالة المعرِّفات لتقديم المعلومات المحددة لهوية الأشخاص المجرَّدة من المعرِّفات في أربع خطوات، على النحو الموضح في الشكل 2 [b-KOREA].

الخطوة 1 الاستعراض الأولي

تتضمن الخطوة 1 التحقق مما إذا كانت البيانات المستهدفة هي معلومات محدِدة لهوية أشخاص أم لا. فإذا كانت تحتوي على هذه المعلومات، انتقل إلى الخطوة 2. إذ تدعو الحاجة إلى إزالة المعرِّفات.

الخطوة 2 إزالة المعرِّفات

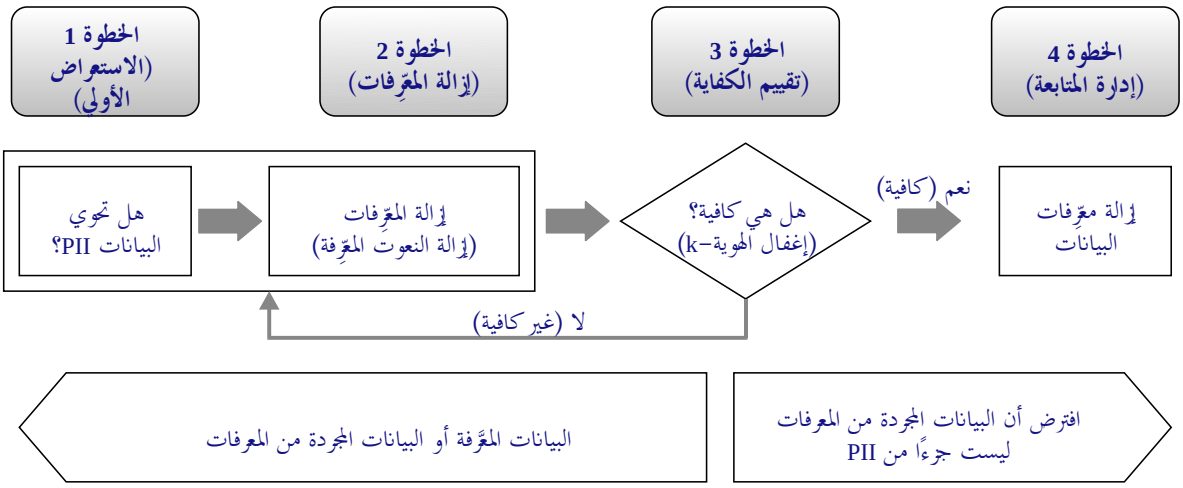
تتضمن الخطوة 2 إزالة معرِّفات البيانات لمنع الاستدلالات على معلومات فردية محددة من مجموعة البيانات المستهدفة. وتستدعي هذه الخطوة أساليب لإزالة عناصر المعلومات المحددة لهوية الأشخاص (PII) أو تحويلها، كلياً أو جزئياً. وتتضمن عناصر المعلومات المحددة لهوية الأشخاص المعرِّفات وشبه المعرِّفات والنعوت الحساسة.

الخطوة 3 تقييم الكفاية

تتضمن الخطوة 3 تقييم مدى كفاية مجموعة البيانات المجرَّدة من المعرِّفات بما فيها عناصر المعلومات المحددة لهوية الأشخاص (PII). وتشمل الاعتبارات ذات الصلة ما إذا كانت مجموعة البيانات المستهدفة لا تزال تحتوي على المعلومات المحددة لهوية الأشخاص، والإمكانية المباشرة لإعادة المعرِّفات، وإمكانية الارتباط التي يمكن أن تؤدي إلى إعادة المعرِّفات.

الخطوة 4 إدارة المتابعة

تتضمن الخطوة 4 قياس السلامة الإدارية والتقنية لمنع إعادة المعرِّفات.



X.1148(20)_F02

الشكل 2 – عملية إزالة المعرِّفات

ويرد مزيد من وصف كل خطوة من هذه الخطوات في الفقرات من 1.7 إلى 4.7.

1.7 الخطوة 1 – الاستعراض الأولي

ينبغي للمنظمات التي تنوي استخدام أو تقديم البيانات لأغراض مختلفة أن تحدد أولاً سياساتها ومعاييرها. ويوصى بأن تتضمن السياسات والمعايير ما يلي:

- ما هو الغرض من المعلومات المجرَّدة من المعرِّفات والغرض من استخدامها؟
- ما نوع نعوت البيانات التي تتكون منها البيانات المجرَّدة من المعرِّفات؟
- ما هي التقنيات المستخدمة لإزالة المعرِّفات؟
- ما هي مستويات المخاطر والآثار السلبية لإعادة المعرِّفات؟
- ما هي الحلول المتاحة في حال إعادة تحديد هوية أشخاص معينين؟
- كيف يقيَّم مستوى إعادة المعرِّفات؟
- كيف تتحدد القوى العاملة اللازمة لإزالة المعرِّفات وكيف تتحدد تكلفتها؟

ويجوز أن تختلف الاعتبارات المحددة التي تشكل الاستعراض الأولي حسب نوع البيانات والغرض المقصود من الاستخدام. ولكن يوصى بوضع مجموعة من المعايير.

يجب على المنظمات التي تنوي معالجة البيانات لعدد من الأغراض الرجوع إلى المعايير المناسبة للتحقق مما إذا كانت البيانات المحددة هي المعلومات المحددة لهوية الأشخاص أم لا. وحتى إن لم تتحدد البيانات على أنها معلومات محددة لهوية أشخاص، يُتطلب من المنظمة النظر في أي إمكانية للربط بين البيانات المتاحة واتخاذ التدابير المناسبة لتقليل هذه المخاطرة. أما إذا تبين أنها معلومات محدِدة لهوية أشخاص، فإن خطوة إزالة المعرِّفات ضرورية.

وتتضمن أمثلة معايير الحكم الخاصة بالمعلومات المحددة لهوية الأشخاص (PII) ما يلي:

- لا توجد قيود خاصة على البيانات بشأن نوعها وشكلها وخصائصها ونسقها؛
- إذا أمكن لمراقب البيانات تحديد هوية فرد باستخدام البيانات، فإن هذه البيانات تعتبر معلومات محدِدة لهوية أشخاص؛
- يجب أن تكون البيانات عن الفرد. أما القيمة الإحصائية لمجموعة تتكون من عدة أفراد فهي ليست معلومات محدِدة لهوية أشخاص (PII)؛

– تعتبر البيانات التي يمكن أن تحدد هوية الفرد من خلال الجمع مع معلومات إضافية معلومات محدِدة لهوية أشخاص. وتشير المعلومات الإضافية عادة إلى المعلومات المتاحة للعموم/بسهولة.

2.7 الخطوة 2 – تطبيق إزالة المعرِّفات

1.2.7 إزالة معرفات المعرِّفات

"المعرّف" هو عبارة عن بيانات من قبيل قيمة أو اسم يُخص بهما فرد أو شيء مرتبط بفرد. وبوجه عام، ينبغي تقليل مجموعة "المعرِّفات" إلى أدنى حد، وينبغي حذف أي معرّفات مضمنة في مجموعات البيانات.

ولكن يمكن أن يتضمن المعرّف الضروري للغاية للغرض المقصود بيانات مثل:

– معرف فريد (رقم التسجيل المقيم، رقم الضمان الاجتماعي (SSN)، رقم جواز السفر، رقم هوية الأجنبي، رقم رخصة القيادة، وما إلى ذلك)؛

– اسم (بالأحرف الصينية، اسم إنكليزي، وما إلى ذلك)؛

– العنوان التفصيلي (رقم المنزل، عنوان الشارع، وما إلى ذلك)؛

– تاريخ (تاريخ الميلاد، الذكرى السنوية (لزفاف، وما إلى ذلك)، تاريخ شهادة، وما إلى ذلك)؛

– رقم الهاتف (المتنقل، في المنزل، المكتب، الفاكس، وما إلى ذلك)؛

– رقم السجل الطبي، رقم التأمين الصحي الوطني، رقم متلقي الرعاية، وما إلى ذلك؛

– رقم الحساب المصرفي، رقم بطاقة الائتمان، وما إلى ذلك؛

– صور (صورة شمسية، فيديو، تسجيل فيديو تلفزيون الدائرة المغلقة (CCTV)، وما إلى ذلك)؛

– البيانات البيومترية (بصمات الأصابع، الصوت، قزحية العين، وما إلى ذلك)؛

– عنوان البريد الإلكتروني، عنوان بروتوكول الإنترنت (IP)، عنوان التحكم في النفاذ إلى الوسائط (MAC)، محدد موقع الموارد الموحد (URL)، وما إلى ذلك؛

– رمز التعريف (رقم الموظف، رقم العميل، وما إلى ذلك)؛

– رقم تعريف فريد آخر (رقم الخدمة العسكرية، رقم تسجيل مصلحة الأعمال، وما إلى ذلك).

2.2.7 إزالة المعرِّفات للنعوت شبه المعرّفة والنعوت شديدة التعريف

بشكل عام، تنبغي إزالة أشباه المعرِّفات المدرجة في مجموعات البيانات إذا كانت غير ذات صلة بالغرض الذي تستخدم البيانات من أجله. وينبغي تطبيق تقنيات إزالة المعرِّفات مثل الاسم المستعار والتجميع إذا كان لشبه المعرف المرتبط باستخدام البيانات عناصر يمكن تحديد هويتها.

ويجب أن تخضع البيانات التي تنطوي على إمكانات شديدة التعريف، مثل المعلومات السلوكية، لإزالة المعرِّفات، وحيثما أمكن، لتقنيات إغفال الهوية.

3.2.7 تقنيات إزالة المعرِّفات

يمكن استخدام مجموعة من التقنيات بما في ذلك الأسماء المستعارة والتجميع وإلغاء البيانات وحجب البيانات بشكل فردي أو في توليفة. وقد لا يكفي تطبيق تقنية الاسم المستعار وحده كتقنية لإزالة المعرِّفات.

وتتوفر أنواع مختلفة من التقنيات بسهولة لتحقيق كل تقنية. وينبغي اختيار الأسلوب الأنسب واستخدامه بناءً على الغرض من استخدام البيانات ونقاط القوة والضعف في كل تقنية معينة. وبمجرد إنجاز عملية إزالة المعرِّفات، يمكن الانتقال إلى الخطوة التالية.

3.7 الخطوة 3 – تقييم الكفاية لعملية إزالة المعرِّفات

يمكن تحديد هوية فرد من خلال الجمع بين البيانات الأخرى أو استخدام تقنيات الاستدلال المختلفة عندما تكون إزالة المعرِّفات غير كافية.

ولتقليل مخاطر إعادة المعرِّفات، تقتضي الضرورة تقييم كفاية البيانات المجرَّدة من المعرِّفات قبل الاستخدام. وهذا يشمل تقييم أسئلة مثل:

- ما هو الغرض من طلب إزالة المعرِّفات هذا؟
- ما نوع نعوت البيانات التي تنطوي عليها إزالة المعرِّفات (بما في ذلك معرِّفات أم لا)؟
- ما هو المستوى المناسب لإزالة المعرِّفات؟

ويمكن إجراء تقييم الكفاية هذا بواسطة مسؤول حماية البيانات (DPO) أو طرف ثالث موثوق (TTP) مفوض أو بواسطة لجنة تقييم خارجية.

ويُستخدم نموذج إغفال الهوية–k من بين نماذج حماية الخصوصية الأخرى عند تقييم الكفاية. ويُعتبر نموذج إغفال الهوية وسيلة أساسية للتقييم. ويمكن إذا لزم الأمر تطبيق نماذج تقييم إضافية (التنوع–l، القرب–t، الخصوصية التفاضلية (DP)، وما إلى ذلك).

راجع الملحق A للاطلاع على تفاصيل إضافية عن تقييم الكفاية.

4.7 الخطوة 4 – إدارة المتابعة

1.4.7 تدابير الحماية للبيانات المجرَّدة من المعرِّفات

تنفَّذ تدابير الحماية لمنع إمكانية إعادة تعريف البيانات المجرَّدة من المعرِّفات إذا تسربت و/أو دُمجت مع بيانات أخرى. وهي تشمل تدابير مثل:

- تدابير الحماية الإدارية: تعيين شخص يتولى المسؤولية عن ملفات البيانات المجرَّدة من المعرِّفات، والبت في تبادل البيانات المجرَّدة من المعرِّفات، وإتلاف البيانات بمجرد تحقيق الغرض من استخدامها؛
- تدابير الحماية التقنية: تقييد النفاذ إلى ملفات البيانات المجرَّدة من المعرِّفات وإدارة سجلات النفاذ وتثبيت برامج الأمن وتشغيلها؛

بالإضافة إلى ذلك، تتضمن الإجراءات الأمنية أيضاً إجراءات وقائية يجب اتخاذها في حال تسرب بيانات مجرَّدة من المعرِّفات. وهي تشمل تدابير مثل:

- تحليل سبب التسرب وتنفيذ تدابير السلامة الإدارية والتقنية لمنع المزيد من التسرب؛
- سحب وإتلاف ما تسرب من البيانات المجرَّدة من المعرِّفات.

2.4.7 مراقبة إمكانيات إعادة المعرِّفات

يجب على مراقب البيانات الذي ينوي استخدام بيانات مجرَّدة من المعرِّفات أو تقديمها لطرف ثالث أن يراقب بانتظام إمكانيات إعادة المعرِّفات.

وعند كشف إمكانية إعادة المعرِّفات، يجب طلب معالجة البيانات وسحبها وإتلافها إلى مراقب البيانات الذي زُود بالبيانات المجرَّدة من المعرِّفات.

3.4.7 متطلبات بشأن التعاقد مع طرف ثالث

يجب تضمين إدارة مخاطر إعادة المعرِّفات في العقد عند تقديم أو تفويض بيانات مجرَّدة من المعرِّفات لطرف ثالث كي يستخدمها. وتتضمن إدارة مخاطر إعادة المعرِّفات ما يلي:

- إبلاغ مواضيع البيانات بالكشف عن البيانات لدى أطراف ثالثة؛

- تقديم بيانات مغفلة الهوية لأطراف ثالثة حيثما أمكن ذلك؛
- حظر إعادة المعرِّفات: يشترط منع مراقب البيانات الذي يعطى بيانات مجرَّدة من المعرِّفات أو يكلَّف بمعالجتها من إعادة تعريف البيانات عن طريق دمجها مع بيانات أخرى؛
- تقييد إعادة التقديم أو إعادة التكليف: يشترط تحديد النطاق المسموح به لإعادة التقديم أو إعادة التكليف في العقد عند تقديم بيانات مجرَّدة من المعرِّفات أو التكليف بمعالجتها؛
- الإبلاغ بشأن مخاطر إعادة المعرِّفات: يشترط الالتزام بالكف عن معالجة البيانات وإبلاغ المرسِل والمرسَل إليه بمسألة إعادة المعرِّفات عند إعادة معرفات البيانات أو عندما تصبح إمكانية إعادة المعرِّفات عالية.

4.4.7 الإجراءات المضادة لإعادة المعرِّفات

في حال إعادة تعريف البيانات المجرَّدة من المعرِّفات، ينبغي الكف عن معالجة البيانات، وينبغي اتخاذ التدابير اللازمة لمنع تسرب المعلومات المحدِدة لهوية أشخاص.

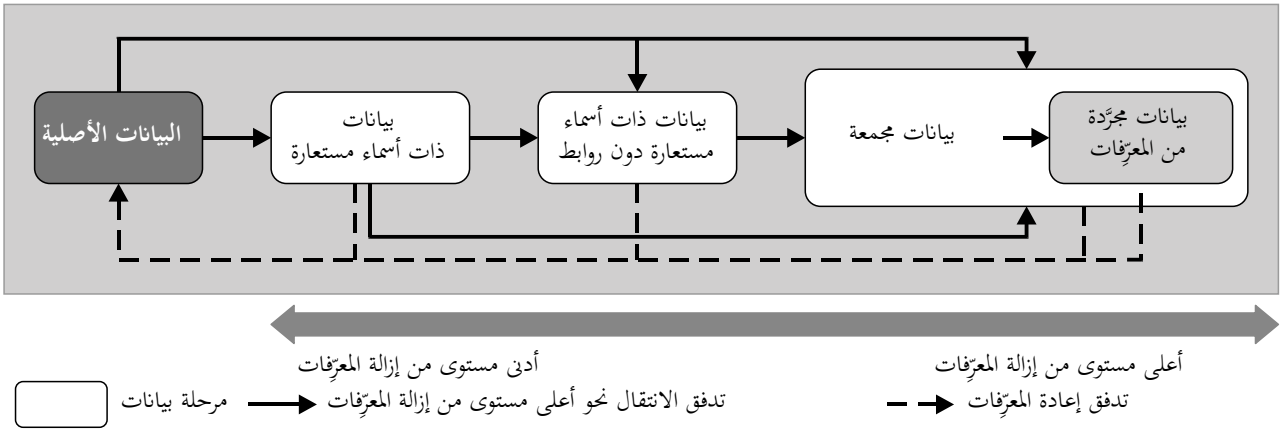
ويجب إتلاف البيانات المعادة معرفاتها على الفور.

8 القيمة الاستعمالية للبيانات المجرَّدة من المعرِّفات

1.8 مراحل البيانات المجرَّدة من المعرِّفات

تعرِّف هذه الفقرة مراحل تجريد البيانات من المعرِّفات التي يمكن تمثيلها على أنها أنواع بيانات لوصف الدرجة التي تتحدد من خلالها هوية الفرد بشكل مباشر من خلال البيانات وكيف يرتبط الفرد بالخصائص (النعوت) في البيانات. وينبغي ألا يتضمن توصيف البيانات في سياق استخدام البيانات أو معالجة البيانات نوع البيانات فحسب، بل يجب أيضاً وصف الدرجة التي يمكن للبيانات من خلالها تحديد هوية فرد أو ربط فرد بمجموعة من الخصائص في البيانات.

ويقدم الشكل 3 مراحل البيانات من البيانات معرَّفة الهوية إلى البيانات المجرَّدة من معرِّفات الهوية في عملية إزالة المعرِّفات. ولكل مرحلة إمكانية مختلفة في طيف مخاطر إعادة المعرِّفات. ويميز نوع البيانات المراحل المحددة التي تمر بها مجموعة البيانات فيما تُزال معرفاتها بشكل متزايد.



الشكل 3 – مراحل البيانات المجرَّدة من المعرِّفات

على النحو المبين في الشكل 3، توجد جميع البيانات في مرحلة إزالة المعرِّفات. فعلى اليمين (أعلى مستوى من إزالة المعرِّفات) توجد بيانات مجرَّدة من المعرِّفات الهوية لا تتعلق بأفراد (من قبيل سجلات الطقس التاريخية) وبالتالي فهي لا تشكل مخاطر للخصوصية. وفي الطرف الأيسر (أدنى مستوى من إزالة المعرِّفات) تتحدد هوية البيانات التي ترتبط مباشرة بأفراد معينين. وما بين مرحلتي البيانات هاتين تقع البيانات التي يمكن ببذل الجهد ربطها، ولا يمكن ربطها إلا بمجموعات من الأشخاص، وهي تستند إلى أفراد ولكن

يتعذر ربطها بهم مرة أخرى. وبشكل عام، صُممت عمليات إزالة المعرِّفات لدفع البيانات إلى اليمين مع حفظ بعض القيمة الاستعمالية المرغوبة، مما يقلل من مخاطر توزيع البيانات المجرَّدة من المعرِّفات على عدد أكبر من السكان أو على عامة الناس.

1.1.8 مرحلة البيانات الأصلية

في المرحلة الأصلية من البيانات معرَّفة الهوية، يمكن ربط البيانات على نحو لا لبس فيه بشخص معين لأن الفرد يمكن رصده في المعلومات. ويمكن العثور على إرشادات بشأن ما يمكن اعتباره معرفات في الفقرة 1.4.4 من المرجع [b-ISO/IEC 29100].

2.1.8 مرحلة البيانات ذات الأسماء المستعارة

في مرحلة البيانات ذات الأسماء المستعارة، يتعذر عكس البيانات بجهود معقولة من أي شخص بخلاف الطرف الذي خصص الاسم المستعار لأن جميع المعرِّفات يستعاض عنها بأسماء مستعارة. ولكن تظل إعادة معرفات البيانات ذات الأسماء المستعارة ممكنة من خلال إمكانية الربط مع البيانات الأخرى.

ويقابل ذلك البيانات المعرفة على أنها بيانات "استخدام اسم مستعار" في الفقرة 14.1.3.

3.1.8 مرحلة البيانات ذات الأسماء المستعارة دون روابط

في مرحلة البيانات ذات الأسماء المستعارة دون روابط، تمحى جميع المعرِّفات أو يستعاض عنها بأسماء مستعارة تمحى لها وظيفة التخصيص أو يحال دون عكسها، بحيث تتعذر إعادة إنشاء الروابط بجهود معقولة من أي شخص بما في ذلك الطرف الذي أقامها. ولكن تظل إعادة معرفات البيانات ذات الأسماء المستعارة دون روابط ممكنة من خلال إمكانية الربط مع البيانات الأخرى.

4.1.8 مرحلة البيانات المجمعة

في مرحلة البيانات المجمعة، تشكل البيانات معلومات عن أشخاص مختلفين بما فيه الكفاية بحيث يتعذر الاستدلال على نعوت على المستوى الفردي لأنها لفيف بيانات إحصائية لا تحتوي على إدخالات على المستوى الفردي. وباستخدام تقنيات التجميع، لا تصل جميع البيانات المجمعة إلى درجة قابلية التعرف تحت عتبة ما إذا كان مقاس الخلية من أجل عبور معين لمجموعة من المتغيرات يمكن أن يقود شخصاً إلى تحديد هوية فرد معين.

ويقابل ذلك البيانات المعرَّفة على أنها "بيانات مجمعة" في الفقرة 1.1.3.

5.1.8 مرحلة البيانات المجرَّدة من المعرِّفات الهوية

في مرحلة البيانات المجرَّدة من المعرِّفات، تُفك روابط البيانات وتُغيَّر النعوت (فتكون قيم النعوت عشوائية أو معممة على سبيل المثال) بحيث يكون هناك مستوى معقول من الثقة بتعذر التعرف على شخص، بشكل مباشر أو غير مباشر، من خلال البيانات وحدها أو بالجمع مع بيانات أخرى.

2.8 نماذج إصدار البيانات

يصنَّف نموذج إصدار البيانات المجرَّدة من المعرِّفات في ثلاثة نماذج وفقاً لحالة سياقات تحليل البيانات [b-UKAN].

هناك ثلاثة نماذج إصدار لتسليم البيانات المجرَّدة من المعرِّفات: عمومي أو شبه عمومي أو غير عمومي.

ويتيح كل نموذج إصدار مستويات مختلفة من تيسر المعلومات وحمايتها. ويمكن أن تختلف جدارة كل نموذج حسب الأغراض و/أو المتطلبات التشريعية لإصدار البيانات. ويؤدي نموذج الإصدار دوراً مهماً في عملية إزالة المعرِّفات، حيث يمكن أن تختلف الكمية المطلوبة من إزالة المعرِّفات حسب نموذج الإصدار المختار.

ويُستعرض كل من نماذج الإصدار الثلاثة في الفقرات من 1.2.8 إلى 3.2.8.

1.2.8 نموذج إصدار البيانات العمومي

في إصدار البيانات العمومي التقليدي، يمكن لأي شخص النفاذ إلى البيانات دون تسجيل أو شروط. وتتضمن الأمثلة على هذه الإصدارات، البيانات المتاحة للجمهور من المنظمات والبيانات المنشورة لفتح النفاذ إلى مستودع بيانات من قبيل بوابة على شبكة الإنترنت. وتقوم المنظمات على نحو استباقي بإصدار مجموعات البيانات وإتاحتها مجاناً لأي شخص ليصار إلى استخدامها وإعادة نشرها.

وعند إصدار البيانات علناً، من الشائع وضع أقل عدد ممكن من القيود على المعلومات، بما في ذلك مَن يمكنه النفاذ إليها وكيف. وعلى هذا النحو، عندما يتعذر تحديد هوية الأفراد الذين يحمِّلون مجموعة البيانات، ينبغي التعامل مع هذه الكشوفات على أنها إصدارات عمومية للبيانات.

وينبغي التعامل معها على أنها إصدارات عمومية للبيانات في الحالات التي لا تتطلب من الشخص الذي يطلب معلومات الموافقة على الأحكام أو الشروط المتعلقة بمعالجة المعلومات أو خصوصيتها أو أمنها، في حالة طلبات النفاذ إلى المعلومات في الفقرة 2.2.8.

2.2.8 نموذج إصدار البيانات شبه العمومي

يعتبر نموذج تبادل البيانات شبه العمومي أكثر تقييداً من نموذج إصدار البيانات العمومي ويحدث عند وجود عملية طلب وموافقة رسمية للنفاذ إلى البيانات. وفي هذه الحالة، يمكن أن يوافق مستلم البيانات على بعض شروط الاستخدام أو أن يوقع على عقد "بالنقر على زر في شاشة حاسوب". وعقود النقر على زر في الشاشة هي شروط استخدام عبر الإنترنت يمكن أن تضع قيوداً على ما يمكن فعله بالبيانات وكيفية التعامل مع البيانات. وبغض النظر عن ذلك، يظل بإمكان أي شخص تحميل مثل هذه البيانات.

ويمكن أن يستفاد من إزالة المعرِّفات أيضاً في الاستجابة لطلبات النفاذ إلى المعلومات الخاصة بمجموعات بيانات. وباستخدام إزالة المعرِّفات، يمكن للمنظمات الاستجابة للطلبات بطريقة تحمي الخصوصية مع الحفاظ على القيمة الاستعمالية للمعلومات. ويمكن للمنظمات استخدام عناصر التحكم في النفاذ لبعض القيود عند تبادل البيانات من خلال نظام معلومات مثل:

- مطالبة جميع المستخدمين بالتسجيل وتقديم معلومات الاتصال قبل النفاذ إلى البيانات؛
- استخدام بروتوكولات الاستيقان للتحقق من هوية الفرد؛
- استخدام أنظمة النفاذ المتدرج لمنح مستويات مختلفة من النفاذ لأطراف مختلفة على أساس انتماءات أو بيانات اعتماد الفرد، على سبيل المثال.

وباستخدام أنظمة المعلومات هذه، تمكن إتاحة نظام استعلام تفاعلي لمجتمع الباحثين، وقد تمكن إتاحة البيانات الخام لعدد صغير من المحللين المعتمدين من خلال عملية غربلة دقيقة.

وأيضاً، تحدث حالة نفاذ إلى البيانات لا تتطلب أي تبادل للبيانات عندما يطلب المحللون أن يقوم مراقب البيانات بإجراء تحليل نيابة عنهم. لذلك، قد لا تنطوي هذه الحالة على تبادل المنظمة للبيانات.

3.2.8 نموذج إصدار البيانات غير العمومي

لا يمكن تبادل مجموعات البيانات التي تحتوي على المعلومات المحدِدة لهوية أشخاص داخل المنظمات وفيما بينها إلا إذا كان الكشف مسموحاً بموجب التوجيه التنظيمي في البلاد. أما إذا كان الكشف غير مسموح وظلت المنظمات ترغب في تبادل مجموعات البيانات، فتجب إزالة أي معلومات محدِدة لهوية أشخاص. وتقدم إصدارات البيانات غير العمومية أقل قدر من التيسر، ولكن قدراً أكبر من الحماية، مما يتطلب قدراً أقل من إزالة المعرِّفات.

وعند تبادل المعلومات بين المنظمات، ونظراً لأن النفاذ إلى مجموعة البيانات يقتصر على منظمة، يمكن وضع المتطلبات المتعلقة بخصوصية المعلومات وأمنها وإنفاذها من خلال اتفاق تبادل البيانات. وللتعامل مع إصدار البيانات على أنه غير عمومي، لا بد من اتفاق لتبادل البيانات بين الطرفين. ويشكل اتفاق تبادل البيانات جزءاً مهماً من إستراتيجية تخفيف المخاطر في هذه الإصدارات، وهو يتضمن بعض المصطلحات الشائعة مثل:

- تحديد المسموح لهم بالنفاذ (ضوابط المتلقي)؛
- متطلبات أمن البيانات (ضوابط البنية التحتية)؛
- قيود على الاستخدام، ولا سيما حظر الربط بملفات أخرى والإعادة المتعمدة للمعرفات (ضوابط البيانات الأخرى والإدارة)؛
- متطلب إتلاف البيانات بمجرد انتهاء الاستخدام (ضوابط الإدارة).

والغرض من اتفاق تبادل البيانات ثلاثي الأبعاد:

- إنه يميز بوضوح بين الأفراد أو المنظمات التي يثق بها مراقب البيانات وتلك التي لا يثق بها؛
- إنه إطار يحدد الشروط التي يمكن أن يحدث فيها النفاذ؛
- يمكنه تحديد العقوبات أو الغرامات في حالة انتهاك الفرد/المنظمة لشروط النفاذ تلك.

4.2.8 مقارنة نماذج إصدار البيانات

في بيئة تدفق البيانات، تتمثل إحدى طرق الحد من فرصة إعادة المعرِّفات في وضع ضوابط للطريقة التي يمكن بها الحصول على البيانات واستخدامها. ويمكن تصنيف هذه الضوابط وفقاً لنماذج إصدار البيانات المختلفة، فلكل منها مزايا ومخاطر مختلفة. ويمكن أن تختار المنظمات أيضاً تطبيق نهج النفاذ المتدرج الذي يجمع بين العديد من هذه النماذج للتعامل مع مجموعة متنوعة من حالات الاستخدام والتهديدات للخصوصية. بالإضافة إلى ذلك، ينبغي أن تنظر نماذج الإصدار في إمكانية الإصدارات المتعددة أو الدورية. وتتراوح العديد من النماذج المسماة بين انعدام القيود والقيود الصارمة. ويقدم الجدول 2 مقارنة بين نماذج إصدار البيانات.

الجدول 2 – مقارنة نماذج إصدار البيانات

	نموذج الإصدار العمومي	نموذج الإصدار شبه العمومي	نموذج الإصدار غير العمومي
حقوق النفاذ	• لكل شخص حق النفاذ إلى البيانات الصادرة بحرية	• النفاذ محصور بفرد أو بمنظمة (أو بمجموعة فرعية منها) إلى البيانات الصادرة	• نفاذ مجموعة فرعية من الأفراد أو المنظمات إلى البيانات الصادرة
حالات الاستخدام	• نفاذ غير مقيد إلى البيانات من خلال بوابة إلكترونية. أي متاح بحرية لأي شخص	• إعداد آمن في الموقع • نفاذ مقدَّم • نفاذ افتراضي عن بعد • نفاذ من خلال مخدِّم التحليل	• تبادل ضمن منظمة وبين المنظمات
الحقوق	• حقوق غير محدودة في إعادة استخدام البيانات وإعادة توزيعها	• متاح لمن يجاز له من أفراد أو منظمات	• تُحظر إعادة استخدام البيانات أو إعادة نشرها أو توزيعها
هجوم إعادة المعرِّفات	• هجوم استعراضي للدعاية	• هجوم متعمد من الداخل • تعرف غير مقصود على فرد في مجموعة البيانات من جانب أحد المعارف • تسرب البيانات	

3.8 العلاقة بين نموذج إصدار البيانات ومرحلة البيانات

1.3.8 نموذج إصدار البيانات غير العمومي

عند إرسال البيانات من مصدر بيانات إلى نموذج إصدار غير عمومي، تتطلب البيانات إزالة المعرِّفات. وفي الظروف العادية، على الرغم من كون نموذج الإصدار غير عمومي، ستُستخدم البيانات ذات الأسماء المستعارة دون روابط وبيانات إزالة المعرِّفات ذات المستوى الأعلى. وفي هذه الحالة، يمكن استخدام أدوات إزالة المعرِّفات مثل الاسم المستعار والتجفير والتركيب والإلغاء وما إلى ذلك.

أما إذا كان هناك عقد أو قانون خاص بين الجانبين، فيمكن استخدام البيانات ذات الأسماء المستعارة لتحليل البيانات وتخزينها خلال هذه المرحلة.

2.3.8 نموذج إصدار البيانات شبه العمومي

عند إرسال البيانات من مصدر بيانات إلى نموذج إصدار شبه عمومي، يحتاج هذا النموذج إلى مستوى أعلى لإزالة المعرِّفات من ذاك في نموذج الإصدار غير العمومي. ويجري هذا النموذج معالجة إحصائية لمنع إعادة المعرِّفات. وبعد ذلك، يمكن إصدار البيانات المجمعة وبيانات إزالة المعرِّفات ذات المستوى الأعلى إلى نموذج الإصدار شبه العمومي. وبعبارة أدق، يمكن استخدام أدوات إزالة معرِّفات مثل الأدوات الإحصائية والعشوائية وما إلى ذلك.

وعلى النحو الموضح في الجدول 2، يمكن السماح بمستوى أقل نسبياً من إزالة المعرِّفات مقارنة بنموذج الإصدار العمومي، حيث لا يمكن النفاذ إلى البيانات إلا للأفراد أو المنظمات المقيّدة.

3.3.8 نموذج إصدار البيانات العمومي

عند إرسال البيانات من مصدر بيانات إلى نموذج إصدار عمومي، تحتاج هذا النموذج إلى مستوى أعلى لإزالة المعرِّفات من ذاك في نموذج الإصدار شبه العمومي. ويجري هذا النموذج العملية للحصول على بيانات إزالة المعرِّفات وبعد هذه العملية، يمكن استخدام النتائج لنموذج الإصدار العمومي، على النحو الموضح في الجدول 2.

الملحق A

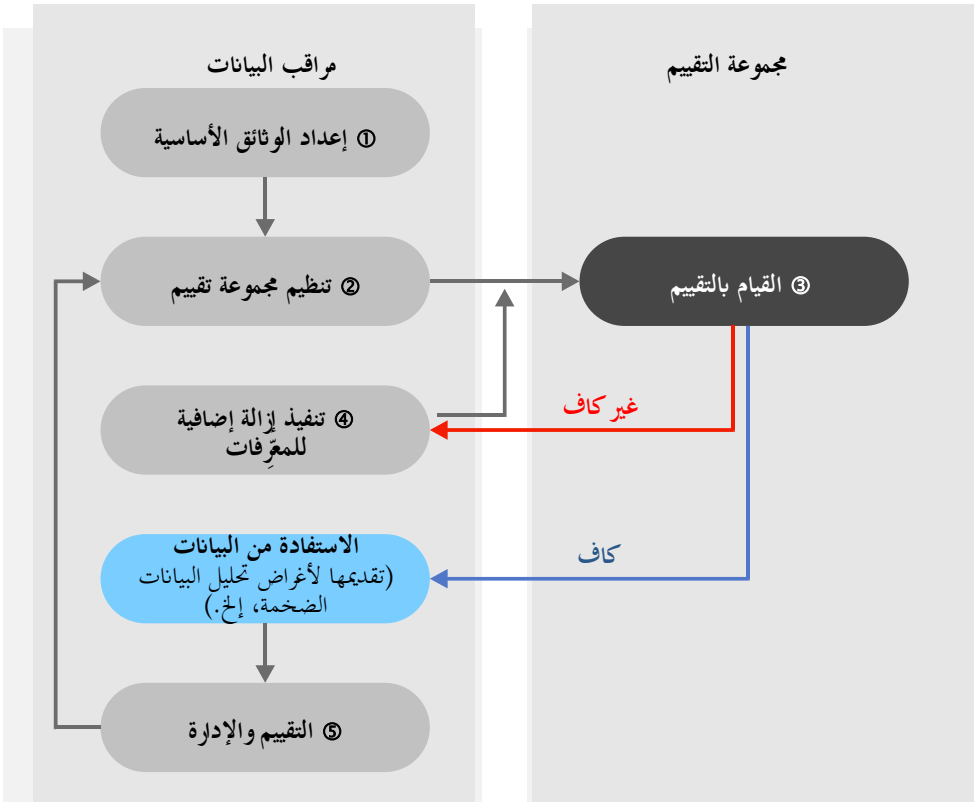
إجراءات تقييم الكفاية

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية.)

يقدم هذا الملحق نموذجاً للقيام بإجراءات تقييم الكفاية [b-KOREA]. انظر الشكل 1.A

فيما يلي خطوات إجراء تقييم الكفاية:

- إعداد الوثائق الأساسية. يقوم مراقب البيانات بإعداد الوثائق الأساسية اللازمة لتقييم الكفاية مثل بيان البيانات وحالة إزالة المعرِّفات ومستوى إدارة المنظمات المستخدمة. وعبارة "المنظمة المستخدمة" تعني أن المنظمة تعتزم استخدام البيانات المجرَّدة من المعرِّفات بعد إزالة المعرِّفات.
- تنظيم مجموعة تقييم. يمكن لمسؤول الخصوصية تشكيل مجموعة التقييم أو استدعاء مسؤول حماية البيانات أو طرف ثالث موثوق لإجراء التقييم.
- إجراء التقييم. تقوم مجموعة التقييم بتقييم مدى كفاية مستوى إزالة المعرِّفات من خلال استخدام الوثائق الأساسية التي أعدها مدير المعلومات المحددة لهوية الأشخاص (PII).
- تنفيذ إزالة إضافية للمعرِّفات. يجب على مراقب البيانات تنفيذ إزالة إضافية للمعرِّفات بالتعبير عن آراء المشاركين في التقييم إذا كانت نتيجة التقييم غير وافية بالغرض منه.
- الاستفادة من البيانات. يمكن استخدام البيانات أو تقديمها لأغراض مثل تحليل البيانات الضخمة إذا بيَّن التقييم كفاية إزالة المعرِّفات.



X.1148(20)_FA.1

الشكل 1.A – تقييم كفاية إجراء إزالة المعرِّفات

1.A إعداد الوثائق الأساسية

يقوم مراقب البيانات بإعداد الوثائق الأساسية اللازمة لتقييم الكفاية مثل بيان بيانات موضوع التقييم وحالة إزالة المعرِّفات ومستوى إدارة المنظمة المستخدمة.

2.A تنظيم مجموعة تقييم

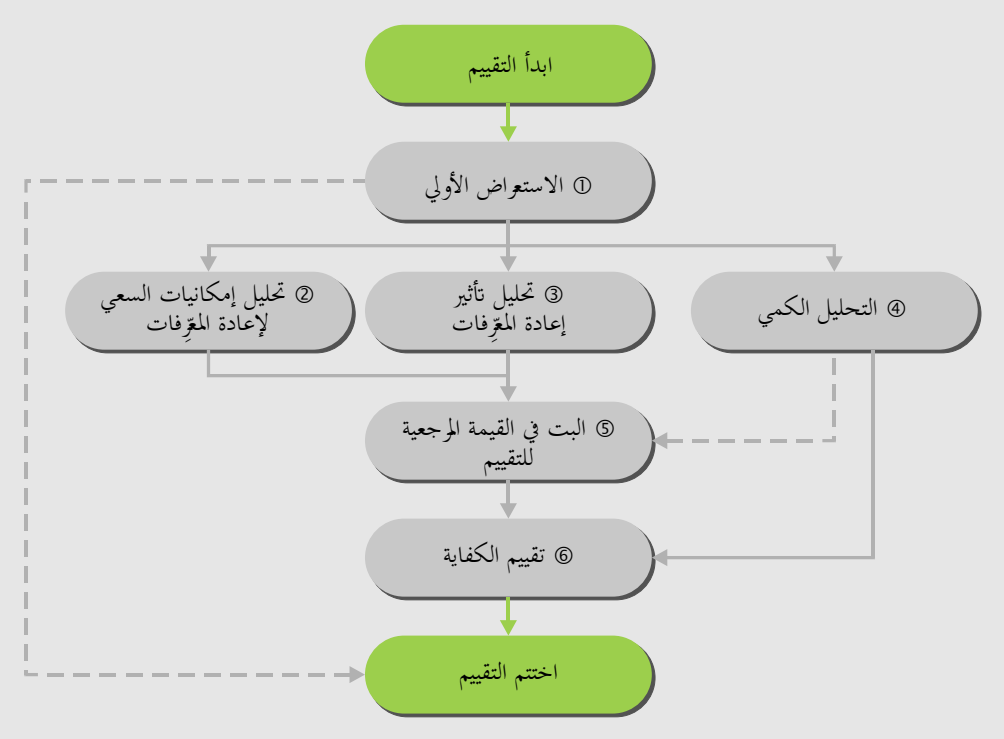
يمكن لمسؤول الخصوصية تشكيل مجموعة التقييم. ويعيَّن أكثر من خبير في الشؤون القانونية وإزالة المعرِّفات من مجموعة خبراء تشغِّلها وكالات متخصصة في كل مجال عند تكليف المهنيين الخارجيين.

وتتكون مجموعة التقييم من أعضاء ليس لديهم مصالح مباشرة في الغرض من استخدام البيانات.

3.A إجراء التقييم

تقوم مجموعة التقييم بتقييم كفاية إزالة المعرِّفات بناءً على الوثائق الأساسية واستخدام نموذج إغفال الهوية–k.

- الاستعراض الأولي. تُستعرض الوثائق الأساسية التي يقوم بإعدادها مراقب البيانات والتحقق منها من خلال المقابلة لمعرفة وجود أو غياب عناصر التعريف بهوية أشخاص في مجموعة البيانات، وما إذا كانت أغراض الاستخدام وتقنيات إزالة المعرِّفات مناسبة.
- تحليل إمكانيات السعي لإعادة المعرِّفات. تحلَّل إمكانيات السعي لإعادة المعرِّفات بما في ذلك النية ومستوى حماية المعلومات المحدِدة لهوية أشخاص وقدرة مراقب البيانات الذي يستخدم البيانات أو يتلقاها.
- تحليل تأثير إعادة المعرِّفات. يقيَّم التأثير المحتمل على موضوع البيانات عند إعادة معرفات البيانات عن قصد أو عن غير قصد.
- التحليل الكمي. يُتحقق من دقة قيمة K المقدمة من مراقب البيانات.
- البت في القيمة المرجعية للتقييم. تحدد مجموعة التقييم القيمة المرجعية للتقييم بشكل شامل إذ ـاخذ في الاعتبار إمكانات إعادة المعرِّفات، وتأثير إعادة المعرِّفات، ونتائج التحليل الكمي، والغرض من استخدام البيانات.
- تقييم الكفاية. يُبت في كفاية إزالة المعرِّفات بمقارنة القيم المحسوبة الناتجة عن متوسط القيمة المرجعية والتحليل الكمي.



X.1148(20)_FA.2

الشكل 2.A – إجراء كفاية التقييم

4.A تدابير إضافية لإزالة المعرِّفات

- يقوم مراقب البيانات بتنفيذ تدابير إضافية لإزالة المعرِّفات بناءً على الملاحظات التقييمية من مجموعة التقييم إذا كانت نتيجة التقييم غير كافية.
- تشرع مجموعة التقييم في إعادة التقييم بمجرد أن يفرغ مراقب البيانات من تنفيذ الإزالة الإضافية للمعرِّفات.

5.A الاستفادة من البيانات

- يستفاد من البيانات المجرَّدة من المعرِّفات في تحليل البيانات الضخمة أو السماح بتقديمها إلى طرف ثالث إذا قُيِّم (أعيد تقييمه) على أنه واف بالغرض.
- من حيث المبدأ، يُحظر تقديم البيانات أو كشفها لمستخدمي البيانات العموميين أو غير المتعاقدين عليها في غياب استراتيجية مناسبة للتخفيف من المخاطر لنماذج إصدار البيانات بسبب ارتفاع مخاطر إعادة المعرِّفات.
- تُتلف البيانات بمجرد تحقيق الغرض من استخدامها أو إن لم تعد هناك حاجة إليها.
- ينبغي الالتزام بخطوات إدارة المتابعة في عملية الاستفادة من البيانات لاستخدامها الفعال في شكل بيانات مجرَّدة من المعرِّفات.

الملحق B

نُهج إزالة المعرِّفات غير المهيكَلة

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية.)

خلافاً لإزالة معرِّفات البيانات المهيكَلة، تطُبّق آليات إزالة المعرِّفات للبيانات غير المهيكَلة على البيانات الخام بدلاً من حقول البيانات المهيكَلة. وفي حالة الصورة أدناه، إزالة المعرِّفات تعني إزالة الوجوه أو الاستعاضة عنها بوجوه أخرى على النحو الموضح في الشكل 1.B.

الشكل 1.B – مثال على إزالة معرِّفات الوجوه

هناك أربعة أنواع من البيانات غير المهيكَلة:

1) بيانات نصية غير مهيكَلة: بيانات الإنترنت، وثيقة تقرير، ومدونة إنترنت، الأخبار، وما إلى ذلك؛

2) بيانات فيديوية غير مهيكَلة: جميع البيانات الفيديوية غير مهيكَلة، وتقدم بعض معلومات الوسم بيانات منظمة؛

3) بيانات سمعية غير مهيكَلة: جميع البيانات السمعية غير مهيكَلة، وتُترجم بعض معلومات الوسم أو المعلومات السمعية المعروفة إلى البيانات النصية؛

4) بيانات السجل غير المهيكلة: بيانات السجل المتولدة آلياً غير مهيكَلة ولكنها تحتوي عادةً على نمط ما وتمكن ترجمتها إلى الشكل المهيكَل.

ولتمثيل المعلومات النحوية للبيانات غير المهيكَلة بما في ذلك النص والصوت والصورة والفيديو، ينبغي أن يحتوي نظام معالجة إزالة المعرِّفات على ثلاث وحدات:

1) وحدة كشف معلومات الوسائط المتعددة لكشف معلومات الشرح النصية من بيانات الوسائط المتعددة المدخلة:
   - تتضمن كاشف كلام يحول المدخلات الصوتية إلى نص لتتبع كائن أو نشاط مدرج في المدخلات الصوتية؛
   - وتتضمن كاشفاً بصرياً للتعرف على الأحرف يستخرج الأحرف من مدخلات الصورة؛
   - وتتضمن كاشفاً بصرياً يستخرج كائناً أو نشاطاً مدرجاً في مدخلات الصورة أو يزيل رسماً من مدخلات صورة ساكنة أو مدخلات صورة متحركة؛
   - وتتضمن كاشف محول بصري إلى جملة يستخرج جملة نصية من مدخلات صورة ساكنة أو صورة متحركة.

2) وحدة تشكيل قائمة على المعارف تقسم المعلومات الشرحية ومعلومات السياق إلى معلومات نحوية تمثل التشكيلة الخارجية والدلالات التي تمثل المعلومات الجوهرية:

- تتضمن المعلومات النحوية معلومات المصدر التي تولد بيانات الوسائط المتعددة، ومعلومات بيانات الوسائط المتعددة التي يولدها المصدر، ومعلومات كشف الكائنات المستخرجة من حيز المعنى؛
- وتتضمن المعلومات الدلالية معلومات الحدث المضمَّنة في حيز المعنى المشكِّل لبيانات الوسائط المتعددة ومعلومات السياق.

3) وحدة إزالة المعرِّفات تزيل المعلومات المحددة لهوية الأشخاص من قاعدة المعارف والمعلومات الشرحية النصية.

والبيانات غير المهيكَلة، وآلية إزالة المعرِّفات، ينبغي أن تحدد المتطلبات ذات الصلة وقوة الأمن على النحو التالي:

- هدف إزالة المعرِّفات: تحديد الكائن المستهدَف الذي تنبغي حمايته بالنسبة إلى التطبيق أو الخدمات عبر الإنترنت؟
- كيفية تنفيذ إزالة المعرِّفات: تحديد الآلية التي ينبغي استخدامها لإزالة المعرِّفات؟ ما هو مستوى إزالة المعرِّفات (ومثال ذلك، الصندوق الأسود، التغطية بالبكسلات، الطمس)؟
- إزالة المعرِّفات مقابل إعادة المعرِّفات: تحديد ضرورة استعادة أو إعادة المعرِّفات. وعندما تتطلب السياسة المرعية صورة أصلية للتحقيق في جريمة، هل تمكن استعادة الصورة المجرَّدة من المعرِّفات؟

التذييل I

أمثلة التقنيات النمطية لإزالة المعرِّفات

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يقدم هذا التذييل بعض الأمثلة والأوصاف لتقنيات إزالة المعرِّفات النموذجية.

1.I أدوات إحصائية لتقنيات إزالة المعرِّفات

- أخذ العينات: عملية تُصدر فيها عينة من مجموعة بيانات كاملة، بدلاً من إصدار كامل مجموعة البيانات. وفي حال إصدار عينة فرعية، يمكن أن يقل احتمال إعادة المعرِّفات.
- التجميع: مجموعة من الدالات الإحصائية التي تنتج القيمة الممثلة لمجموعة بيانات كاملة.

2.I أدوات تجفيرية لتقنيات إزالة المعرِّفات

- التجفير القطعي [b-ISO/IEC 11770]: مخطط تجفير ينتج دائماً نفس النص المشفر لنص عادي ومفتاحاً على عمليات تنفيذ منفصلة لخوارزمية التجفير.
- التجفير الحافظ للترتيب [b-AGRAWAL]: مخطط تجفير يُحفظ فيه الترتيب العددي للنصوص العادية.
- التجفير المتماثل [b-ISO/IEC 18033-6]: مخطط تجفير يسمح بإجراء العمليات الحسابية على نص مشفر، ومن ثم بتوليد نتيجة مجفرة تتطابق مع نتيجة العمليات الجارية على النص العادي، عند فك تجفيرها.
- التجفير الحافظ للنسق [b-NIST 800-38G]: مخطط تجفير يكون فيه نص التشفير بنفس نسق النص العادي.
- السر المشترَك المتماثل [b-ISO/IEC 18033-6]: نوع من خوارزمية التشارك في سر يجفَّر فيه السر باستخدام تجفير متماثل.

3.I تقنيات الإلغاء

- الحجب: عملية تبديل حقل بقيمة أو إزالته. ومن أمثلة تقنية الإلغاء، تبديل رقم هاتف بعلامات نجمية أو باسم مستعار متولد عشوائياً.
- الإلغاء المحلي: عملية تلغي أو تزيل قيماً محددة للنعوت من السجلات المختارة. وتؤدي إزالة البيانات إلى تعزيز حماية الخصوصية ولكنها يمكن أن تقلل من القيمة الاستعمالية لمجموعة البيانات.
- إلغاء السجلات: عملية تنطوي على إزالة سجل كامل أو سجلات كاملة من مجموعة بيانات.

4.I تقنيات استخدام الأسماء المستعارة

عملية تزيل الارتباط بموضوع البيانات وتضيف ارتباطاً بين مجموعة معينة من الخصائص المتعلقة بموضوع البيانات وواحد أو أكثر من الأسماء المستعارة. وعادةً ما ينفَّذ اسم مستعار بالاستعاضة عن المعرِّفات المباشرة باسم مستعار، من قبيل قيمة متولدة عشوائياً. وتتضمن أمثلة المعرِّفات المباشرة الأسماء وعناوين البريد الإلكتروني والأرقام الصادرة عن الحكومة. ويستعاض عن جميع المعرِّفات المباشرة والنعوت الإضافية المحتملة أو جميع النعوت المعرِّفة المتبقية باسم مستعار.

5.I تقنيات التعميم

- التدوير: عملية الاستعاضة عن قيمة عددية بقيمة أخرى مساوية لها تقريباً ولكن بتمثيل أقصر أو أبسط أو أكثر وضوحاً.
- تشفير القمة والقاع: عملية يُضبط فيها النعت الذي تتجاوز قيمه الحد الأعلى (أو الحد الأدنى) كعتبة للقيمة الكبرى (أو الصغرى) الممكنة.

6.I تقنيات التوزيع العشوائي

- إضافة الضوضاء: عملية تضاف فيها قيمة عشوائية لا يمكن التنبؤ بها إلى نعت مختار لمجموعة بيانات.
- التقليب: عملية تبادل قيم النعت المختار عبر السجلات في مجموعة بيانات دون تعديل.
- التجميع الصِغري: عملية يستعاض فيها عن جميع قيم النعوت المستمرة بمتوسطاتها المحسوبة بطريقة خوارزمية معينة.

7.I البيانات المركبة

البيانات المركبة هي نهج ينتج بشكل مصطنع بيانات صغرية لتمثيل نموذج بيانات إحصائي معرَّف مسبقاً. وبحكم التعريف، لا تحتوي مجموعات البيانات المركبة على بيانات جرى جمعها من مواضيع البيانات القائمة، لكنها تبدو حقيقية للغرض المقصود.

التذييل II

نُهج عملية إزالة المعرِّفات

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يقدم هذا التذييل بعض الأمثلة والتفاصيل لنُهج عملية إزالة المعرِّفات.

1.II نُهج إزالة المعرِّفات المتمحور حول البيانات

بالنظر إلى أن تقنيات إزالة المعرِّفات تعدل البيانات الأصلية لمنع كشف المعلومات المحددة لهوية الأشخاص، ينشأ توتر واضح بين القيمة الاستعمالية والخصوصية. ويكمن التحدي في حماية الخصوصية بالحد الأدنى من فقدان الدقة: فمن الناحية المثالية، ينبغي لمستخدمي البيانات تشغيل تحليلاتهم على البيانات المجرَّدة من المعرِّفات دون فقدان الدقة فيما يتعلق بنتائج تلك التحليلات عند تشغيلها على البيانات الأصلية.

وتصعب عملياً إزالة المعرِّفات تماماً دون المساس بالقيمة الاستعمالية لمجموعة البيانات. وفي البيانات الضخمة، تتفاقم هذه المشكلة بسبب كمية البيانات وتنوعها. فمن ناحية، عادة ما تكون إزالة المعرِّفات منخفضة المستوى (من قبيل الاكتفاء بإزالة المعرِّفات من خلال إلغاء المعرِّفات المباشرة) وهي غير كافية لضمان إزالة المعرِّفات. ومن ناحية أخرى، قد يمنع الشطط في إزالة المعرِّفات ربط البيانات التي تأتي من مصادر مختلفة عن نفس الشخص (أو الأفراد المشابهين له)، وبالتالي تُحبَط العديد من الفوائد المحتملة للبيانات الضخمة.

وتصف هذه الفقرة نهجين لإزالة معرِّفات تركز على البيانات للتعامل مع التوتر بين القيمة الاستعمالية والخصوصية. ويمكن استخدام مقاييس القيمة الاستعمالية العامة والخاصة باستخدام البيانات لمعالجة كيفية قياس القيمة الاستعمالية لمجموعة بيانات صادرة مجرَّدة من المعرِّفات.

1.1.II نهج القيمة الاستعمالية أولاً لإزالة المعرِّفات

في البيانات الضخمة، كثيراً ما تُجمع المعلومات عن الفرد من عدة مصادر مستقلة. وبالتالي، تعد القدرة على الربط بين السجلات التي تنتمي إلى نفس الشخص (أو من نفس النوع/مماثل له) أمراً محورياً في إنشاء البيانات الضخمة.

وفي نهج القيمة الاستعمالية أولاً لإزالة المعرِّفات، تشغَّل على مجموعة البيانات الصغرية تقنية إزالة المعرِّفات باختيار معلمة ارشادية ذات خصائص مناسبة لصون القيمة الاستعمالية، وبعد ذلك، يقاس خطر الكشف. لذلك، فإن نهج القيمة الاستعمالية أولاً لإزالة المعرِّفات بطيء ويفتقر إلى الضمانات الرسمية للخصوصية. على سبيل المثال، يمكن تقدير خطر إعادة المعرِّفات تجريبياً من خلال محاولة ربط السجلات بين مجموعات البيانات الأصلية وتلك المجرَّدة من المعرِّفات. فإذا اعتبرت المخاطر الحالية عالية جداً، تجب إعادة تشغيل تقنية إزالة المعرِّفات بمعلمات أكثر تشدداً بشأن الخصوصية وربما مع المزيد من التضحية بالقيمة الاستعمالية، ومع تغيير المعلمات بشكل متكرر إلى أن تنخفض مخاطر الكشف التجريبية بما يكفي، كدأب الإحصاءات الرسمية.

وبالطبع، في حين أن إمكانية الربط مرغوبة من منظور القيمة الاستعمالية، إلا أنها تشكل أيضاً تهديداً للخصوصية: وينبغي أن تقل دقة الروابط كثيراً في مجموعات البيانات المجرَّدة من المعرِّفات عنها في مجموعات البيانات الأصلية. ويحدد مقدار قابلية الربط المتوافق مع تقنية إزالة المعرِّفات أو مع نموذج خصوصية إزالة المعرِّفات ما إذا كان يمكن للمحلل أن يربط بشكل مستقل البيانات المجرَّدة من المعرِّفات (بموجب تلك التقنية/النموذج) التي تقابل نفس الفرد، وكيف يمكن للمحلل القيام بذلك.

2.1.II نهج الخصوصية أولاً لإزالة المعرِّفات

يجري إنفاذ نهج الخصوصية أولاً لإزالة المعرِّفات بمعلمة تضمن الحد الأعلى للمخاطر المهددة لكشف إعادة التعريف وربما أيضاً مخاطر كشف النعت. ويتحقق إنفاذ النموذج باستخدام تقنية إزالة معرِّفات خاصة بنموذج ذي معلمات مشتقة من معلمات النموذج. وتتضمن نماذج الخصوصية المعروفة جيداً إغفال الهوية–k وتوسعاته، فضلاً عن الخصوصية التفاضلية وكثيراً ما تؤدي إلى ضعف القيمة الاستعمالية للبيانات/قابلية الربط.

وفي نهج الخصوصية أولاً لإزالة المعرِّفات، إذا انخفضت كثيراً القيمة الاستعمالية الناتجة للبيانات المجرَّدة من المعرِّفات، ينبغي آنئذٍ إما إنفاذ نموذج الخصوصية المستخدَم بتقنية بديلة لإزالة المعرِّفات تكون أقل ضرراً للقيمة الاستعمالية، أو اختيار معلمة خصوصية أقل تشدداً، أو حتى اللجوء إلى نموذج خصوصية مختلف لإزالة المعرِّفات.

2.II نهج إزالة المعرِّفات المتمحور حول الأدوار

تصف هذه الفقرة ثلاثة أنواع من النُهج التي تؤدي أدوار ومسؤوليات بعضها البعض في عملية إزالة المعرِّفات. ويمكن وصف النهج الذي يركز على الأدوار عموماً بإجابته على أسئلة "من" و"ماذا" و"أين وكيف":

- من لديه حق النفاذ إلى البيانات؟
- ما هي التحليلات التي يجوز أو لا يجوز إجراؤها؟
- من أين النفاذ إلى البيانات/تحليلها وكيف الحصول عليه؟

1.2.II إزالة المعرِّفات المركزية

تركز عملية التحكم في الكشف الإحصائي على الإزالة المركزية للمعرِّفات التي يقوم بها مراقب البيانات القادر على النفاذ إلى مجموعة البيانات الأصلية كلها. ولهذا النهج المركزي بعض المزايا والعيوب على النحو الموضح في الجدول 1.II.

الجدول 1.II – خصائص الإزالة المركزية للمعرِّفات

	التفاصيل
المزايا	• لا يحتاج الأفراد إلى إزالة معرِّفات سجلات البيانات التي يقدمونها. ويمكن توقع أن يقوم مراقب البيانات، الذي لديه المزيد من الموارد الحسابية وربما خبرة أكبر، بإزالة المعرِّفات من مجموعة البيانات كلها بشكل واف بالغرض. • لدى مراقب البيانات نظرة شاملة على مجموعة البيانات الأصلية، وبالتالي فهو في أفضل وضع لتحقيق المفاضلة المثلى بين القيمة الاستعمالية للبيانات ومخاطر الإفشاء الماثلة.
العيوب	• يجب أن تثق جميع الأطراف التي تقدم بيانات أصلية في مراقب البيانات (لأن المراقب يمكنه النفاذ إلى جميع البيانات الأصلية). وفي حين أن هذه ليست مشكلة في الإحصاءات الرسمية، حيث يكون مراقب البيانات معهداً إحصائياً وطنياً، فقد تشكل عقبة رئيسية في سيناريو البيانات الضخمة النمطي، ومثال ذلك عندما يكون مراقب البيانات الذي يجمع العديد من مصادر البيانات مجرد شركة خاصة (سمسار بيانات على سبيل المثال). • خاصةً في حالة البيانات الضخمة، يمكن أن تشكل إزالة المعرِّفات عبئاً ثقيلاً للغاية على مراقب واحد. • يشارك العديد من المراقبين في سيناريو واحد لمعالجة البيانات الضخمة، مما يجعل النهج المركزي غير قابل للإدارة.

وتُتمم نُهج إزالة المعرِّفات المحلية وإزالة المعرِّفات التعاونية المزايا والعيوب المذكورة أعلاه.

2.2.II إزالة المعرِّفات المحلية

تشكل إزالة المعرِّفات المحلية نهجاً بديلاً لتقييد الإفشاء يناسب السيناريوهات (بما في ذلك البيانات الضخمة) التي لا يثق فيها الأفراد (مواضيع البيانات) (أو يثقون جزئياً فقط) بمراقب البيانات الذي يجمع البيانات. فيقوم كل شخص بإزالة معرفات بياناته قبل تسليمها إلى مراقب البيانات.

وبأخذ حماية الخصوصية في الاعتبار، تنبغي إزالة معرفات البيانات التي جمعها مصدر معين في المصدر قبل إتاحتها. ولكن الإزالة المستقلة للمعرِّفات من جانب كل مصدر تنطوي على خسارة في المعلومات أكثر مما هو الحال في الإزالة المركزية للمعرِّفات لأن

الأشخاص يزيلون معرفات بياناتهم دون رؤية بيانات مواضيع أخرى. أي أن المواضيع تفتقر إلى نظرة شاملة على مجموعة البيانات، مما يجعل يصعب عليها إيجاد مفاضلة جيدة بين الحد المتحقق من مخاطر الكشف وبين خسارة المعلومات المتكبّدة.

3.2.II إزالة المعرِّفات التعاونية

تجمع عملية إزالة المعرِّفات التعاونية بين قلة خسارة القيمة الاستعمالية للإزالة المركزية للمعرِّفات وبين الدرجة العالية من حفظ خصوصية الشخص في الإزالة المحلية للمعرِّفات. وتتمثل مشكلة الإزالة المركزية للمعرِّفات في أن موضوع البيانات إن لم يثق في مراقب البيانات بشأن استخدامه و/أو إزالته لمعرفات بياناته بشكل سليم، يمكن أن يقرر تقديم بيانات خاطئة (فيتسبب بالتالي في تحيز الإجابة) أو عدم تقديم بيانات على الإطلاق (فيتسبب بالتالي في تحيز الإجابة). لذلك، يمكن للمواضيع التعاون لتحديد مخاطر الكشف المرتبطة ببياناتهم ثم تطبيق المستوى المناسب من الحماية محلياً بطريقة موزعة وتعاونية، تسعى إلى تحقق خاصيتين رئيسيتين:

- عدم التسبب في خسارة معلومات أكثر من مجموعة البيانات التي تحصَّل باستخدام النهج المركزي لمستوى الخصوصية نفسه. ويتفوق ذلك على النهج المحلي في أنه يقلل من خسارة المعلومات.
- لا تكتسب مواضيع البيانات ولا مراقب البيانات مزيداً من المعرفة عن النعوت المكتومة لأي موضوع بيانات محدد آخر بخلاف المعرفة الموجودة في مجموعة البيانات النهائية المجرَّدة من المعرِّفات. ويتفوق ذلك على النهج المركزي من خلال حفظ الخصوصية أيضاً إزاء جامع البيانات.

بالإضافة إلى ذلك، يمكن أن يؤدي النهج التعاوني إلى بروتوكولات تعمل بسلاسة بدون آليات إنفاذ خارجية. ففي إزالة معرفات البيانات الصغرية، تؤثر حماية الخصوصية التي يحصل عليها شخص ما على حماية الخصوصية التي يحصل عليها الآخرون. ولتحسين القيمة الاستعمالية المشتركة في النهج التعاوني، يلزم تحويل آمن متعدد الأطراف للبروتوكولات الإلكترونية التي تمكن طرفين أو أكثر من تنفيذ تحويل يتضمن مجموعات بيانات كل منهم بطريقة لا يحتاج فيها أي طرف إلى تسليم مجموعة بيانات صراحة إلى أي من الأطراف الأخرى. ونظراً لأن التحويل الآمن متعدد الأطراف يسمح بتحويل الاستعلامات دون الحاجة إلى مركزية تخزين كل البيانات، فإنه يقلل من الضرر الناتج عن خرق البيانات، ويسمح بالحسابات عبر الأطراف التي لا تثق تماماً في بعضها البعض. ويمكن أن تحسن الحسابات المتعددة الأطراف حفظ الخصوصية والقيمة الاستعمالية في سياقات معينة.

بيبليوغرافيا

[b-ISO/IEC 11770] ISO/IEC 11770 (all parts), *Information technology – Security techniques – Key management*.

[b-ISO/IEC 18033-6] ISO/IEC 18033-6, *Information technology security techniques – Encryption algorithms – Part 6: Homomorphic encryption*.

[b-ISO/IEC 20889] ISO/IEC 20889 (2018), *Privacy enhancing data de-identification terminology and classification of techniques*.

[b-ISO/IEC 27001] ISO/IEC 27001 (2018), *Information technology – Security technique – Information security management systems*.

[b-ISO/IEC 29100] ISO/IEC 29100 (2011), *Information technology – Security technique – Privacy framework.*

[b-NIST 800-38G] NIST Special Publication 800-38G (2016), *Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption.*

[b-NISTIR 8053] NISTIR 8053 (2015), *De-Identification of Personal Information.*

[b-AGRAWAL] Agrawal, R., Kiernan, J., Srikant, R., and Xu, Y. (2004), *Order preserving encryption for numeric data, SIGMOD '04 Proceedings of the 2004 ACM SIGMOD international conference on Management of data, Paris, France, June, pp 563-574.*

[b-KOREA] Korean Ministry of the Interior, *Guidelines on De-identification Measures, June 2016.*
<http://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000821178&fileSn=2&nttId=7187&toolVer=&toolCntKey_>
Last accessed 26 July 2019)
<https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000827161&fileSn=0>
(English, last accessed 12 December 2020)

[b-UKAN] UK Anonymization Network, *The anonymisation decision-making framework, 2016*
<https://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf>

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2021